PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-215351
(43)Date of publication of application : 06.08.1999

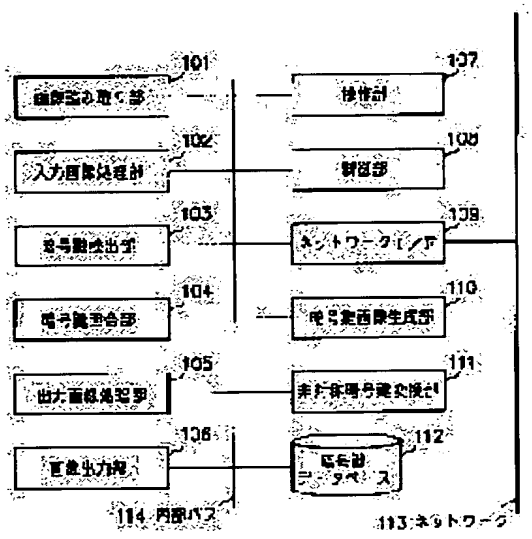
(51)Int.CI. H04N 1/387
B41J 5/30
B41J 29/38
G03G 21/00
G09C 1/00
G09C 1/00
G09C 5/00
H04L 9/32
H04N 1/00
H04N 1/40

(21)Application number : 10-011209
(22)Date of filing : 23.01.1998

(71)Applicant : CANON INC
(72)Inventor : NAMIGATA TAKESHI

(54) IMAGE PROCESSOR AND IMAGE PROCESSING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To inhibit recopying to any one except for a specified person even though an image is viewed similar to a regular copied object by outputting one inputted key on a paper medium at copying operation so that it is hardly conspicuous to human eyes.
SOLUTION: An operation part 107 requests the selection of the open key of an opposite party, to which a recopying operation is permitted, to a user. The open key selected by the user is sent to a password key image generation part 110, it is converted into a 8×8 matrix image and is sent to an output image processing part 105. A prescribed image processing is executed on the picture signal of an original, which is read by an image read part 101, in an input image processing part 102. An output image processing part 105 sends the dot pattern of the open key supplied from the password image generation part 110 and the picture signals of the original supplied from the input image processing part 102, outputs the image of the paper medium and generates the copied object. At copying, open key data of a specified person is embedded into the copied object, so that it becomes hardly conspicuous to the human eyes.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－215351

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	FI		
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		
Ｂ４１Ｊ　5/30		Ｂ４１Ｊ　5/30		Ｃ
29/38		29/38		Ｚ
Ｇ０３Ｇ　21/00	５６２	Ｇ０３Ｇ　21/00	５６２	
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ	

審査請求　未請求　請求項の数８　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平10－11209

(22)出願日　平成10年(1998)１月23日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　波潟　健
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

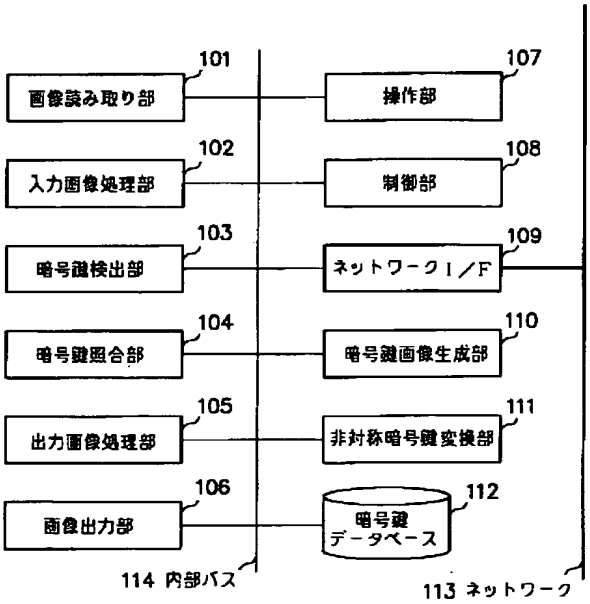
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　画像処理装置および画像処理システム

(57)【要約】

【課題】　一目で文書の内容は分かるが複写行為自体は禁止するというような程度の軽いセキュリティを実現する。

【解決手段】　非対称公開鍵暗号方式に基づく公開鍵を、複写動作時に紙媒体上に人間の視覚には目立ちにくい形で埋め込む暗号鍵画像生成部１１０を設けることにより、複写物を見ること自体はできるが、その複写物をさらに複写しようとする際には、埋め込まれた公開鍵に対応する秘密鍵がなければ複写することができないする。



1

【特許請求の範囲】

【請求項１】　紙媒体上の画像を読み取る画像読取手段を持ち、該画像読取手段により読み取られた画像信号、または外部から入力された画像信号を紙媒体上に出力する手段を持つ画像処理装置であって、

非対称暗号方式に基づく一方の鍵を入力するための鍵入力手段と、

上記入力された一方の鍵を、複写動作時に紙媒体上に人間の視覚には目立ちにくい形で出力する出力手段とを備えたことを特徴とする画像処理装置。

【請求項２】　上記紙媒体上に出力する一方の鍵は、公開鍵暗号方式に基づく公開鍵であることを特徴とする請求項１に記載の画像処理装置。

【請求項３】　上記公開鍵暗号方式に基づく秘密鍵と公開鍵とを互いに対応付けて記憶することにより、暗号鍵の対応を保持する暗号鍵データベース手段を備え、

上記鍵入力手段は、上記暗号鍵データベース手段より提示される公開鍵の一覧から任意の公開鍵を選択することによって上記公開鍵を入力することを特徴とする請求項２に記載の画像処理装置。

【請求項４】　上記公開鍵暗号方式に基づく秘密鍵を入力するための第２の鍵入力手段と、

上記入力された秘密鍵から公開鍵への変換を行う鍵変換手段とを備え、

上記暗号鍵データベース手段は、上記入力された秘密鍵およびそれが変換された公開鍵を対応付けて記憶することを特徴とする請求項３に記載の画像処理装置。

【請求項５】　上記公開鍵が埋め込まれて生成された複写物に対し、複写動作時に、上記埋め込まれた公開鍵に対応する秘密鍵が入力されたかどうかを上記暗号鍵データベース手段を用いて照合する暗号鍵照合手段と、

上記暗号鍵照合手段による照合の結果に応じて複写動作の制御を行う複写制御手段とを備えたことを特徴とする請求項４に記載の画像処理装置。

【請求項６】　上記非対称暗号方式に基づく一方の鍵を上記紙媒体上に複数埋め込むことが可能なように構成したことを特徴とする請求項１～５の何れか１項に記載の画像処理装置。

【請求項７】　上記秘密鍵をネットワーク上で送受信するための通信手段を更に備え、

上記ネットワークを介して外部より入力された秘密鍵を上記鍵変換手段に供給するようにしたことを特徴とする請求項１～６の何れか１項に記載の画像処理装置。

【請求項８】　紙媒体上の画像を読み取る画像読取手段を持ち、該画像読取手段により読み取られた画像信号、または外部から入力された画像信号を紙媒体上に出力する手段を持つ画像処理装置がネットワーク上に接続された画像処理システムであって、

非対称公開鍵暗号方式に基づく秘密鍵を入力するための秘密鍵入力手段と、

2

上記入力された秘密鍵から公開鍵への変換を行う鍵変換手段と、

上記入力された秘密鍵およびそれが変換された公開鍵を対応付けて記憶することにより、暗号鍵の対応を保持する暗号鍵データベース手段と、

上記暗号鍵データベース手段より提示される公開鍵の一覧から任意の公開鍵を選択することによって上記公開鍵を入力する公開鍵入力手段と、

上記入力された公開鍵を、複写動作時に紙媒体上に人間の視覚には目立ちにくい形で出力する出力手段と、

上記公開鍵が埋め込まれて生成された複写物に対し、その後の複写動作時に、上記埋め込まれた公開鍵に対応する秘密鍵が入力されたかどうかを上記暗号鍵データベース手段を用いて照合する暗号鍵照合手段と、

上記暗号鍵照合手段による照合の結果に応じて複写動作の制御を行う複写制御手段と、

上記秘密鍵を上記ネットワーク上で送受信する通信手段とを備え、

上記ネットワークを介して外部より入力された秘密鍵を上記鍵変換手段に供給するようにしたことを特徴とする画像処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は画像処理装置および画像処理システムに関し、特に、非対称暗号鍵方式を利用して複写行為を制限するように構成した複写機および複写機システムに用いて好適なものである。

【０００２】

【従来の技術】近年、社内の機密文書やプライバシーに係る文書など、内容が漏洩しては困るドキュメント等に対して不正な複写行為に対するセキュリティをかける技術開発が盛んになってきている。それには様々な方法があるが、代表的なものとして、特開平６－１４１１９２号公報のように複写内容を暗号化するものなどが知られている。

【０００３】

【発明が解決しようとする課題】しかしながら、この種の技術の場合、正当に文書を利用できる者であっても、暗号化された文書は一旦復号化しなければ内容が分からないという問題があった。また、復号化した文書は再度複写可能となるので、第三者が不正な複写を行うことも可能になってしまうという問題もあった。さらに、この種の技術では、一目で文書の内容は分かるが複写行為自体は禁止したいというような程度の軽いセキュリティには対応できないという問題もあった。

【０００４】本発明は、このような問題を解決するために成されたものであり、何れの人間に対しても通常の複写物に同様に見えながらも、特定の人間以外には再複写を有効に禁止できるようにすることを目的とする。

【０００５】

【課題を解決するための手段】本発明の画像処理装置は、紙媒体上の画像を読み取る画像読取手段を持ち、該画像読取手段により読み取られた画像信号、または外部から入力された画像信号を紙媒体上に出力する手段を持つ画像処理装置であって、非対称暗号方式に基づく一方の鍵を入力するための鍵入力手段と、上記入力された一方の鍵を、複写動作時に紙媒体上に人間の視覚には目立ちにくい形で出力する出力手段とを備える。

【０００６】ここで、紙媒体上に出力する一方の鍵は、公開鍵暗号方式に基づく公開鍵であっても良い。また、公開鍵暗号方式に基づく秘密鍵と公開鍵とを互いに対応付けて記憶することにより、暗号鍵の対応を保持する暗号鍵データベース手段を備え、鍵入力手段は、暗号鍵データベース手段より提示される公開鍵の一覧から任意の公開鍵を選択することによって公開鍵を入力するものであっても良い。また、公開鍵暗号方式に基づく秘密鍵を入力するための第２の鍵入力手段と、入力された秘密鍵から公開鍵への変換を行う鍵変換手段とを備え、暗号鍵データベース手段は、入力された秘密鍵およびそれが変換された公開鍵を対応付けて記憶するものであっても良い。

【０００７】さらに、公開鍵が埋め込まれて生成された複写物に対し、複写動作時に、埋め込まれた公開鍵に対応する秘密鍵が入力されたかどうかを暗号鍵データベース手段を用いて照合する暗号鍵照合手段と、暗号鍵照合手段による照合の結果に応じて複写動作の制御を行う複写制御手段とを更に備えても良い。また、非対称暗号方式に基づく一方の鍵を紙媒体上に複数埋め込むことが可能なように構成しても良い。また、秘密鍵をネットワーク上で送受信するための通信手段を更に備え、ネットワークを介して外部より入力された秘密鍵を上記鍵変換手段に供給するようにしても良い。

【０００８】本発明の画像処理システムは、紙媒体上の画像を読み取る画像読取手段を持ち、該画像読取手段により読み取られた画像信号、または外部から入力された画像信号を紙媒体上に出力する手段を持つ画像処理装置がネットワーク上に接続された画像処理システムであって、非対称公開鍵暗号方式に基づく秘密鍵を入力するための秘密鍵入力手段と、上記入力された秘密鍵から公開鍵への変換を行う鍵変換手段と、上記入力された秘密鍵およびそれが変換された公開鍵を対応付けて記憶することにより、暗号鍵の対応を保持する暗号鍵データベース手段と、上記暗号鍵データベース手段より提示される公開鍵の一覧から任意の公開鍵を選択することによって上記公開鍵を入力する公開鍵入力手段と、上記入力された公開鍵を、複写動作時に紙媒体上に人間の視覚には目立ちにくい形で出力する出力手段と、上記公開鍵が埋め込まれて生成された複写物に対し、その後の複写動作時に、上記埋め込まれた公開鍵に対応する秘密鍵が入力されたかどうかを上記暗号鍵データベース手段を用いて照合する暗号鍵照合手段と、上記暗号鍵照合手段による照合の結果に応じて複写動作の制御を行う複写制御手段と、上記秘密鍵を上記ネットワーク上で送受信する通信手段とを備え、上記ネットワークを介して外部より入力された秘密鍵を上記鍵変換手段に供給するようにしたことを特徴とする。

【０００９】

【発明の実施の形態】本実施形態は、公開鍵暗号方式における公開鍵と秘密鍵との関係を用いて、複写物の再複写許可および再複写禁止を行う例である。

【００１０】暗号方式には、大きく分けて共通鍵（対象）暗号方式と公開鍵（非対称）暗号方式とがある。共通鍵暗号方式では、暗号化する鍵と復号化する鍵とが同じで、送信者と受信者との間で鍵を秘密に保持する必要がある。これに対して、公開鍵暗号方式では、暗号化する鍵と復号化する鍵とが互いに異なり、一方を秘密に保持し（秘密鍵）、もう一方を公開しておく（公開鍵）ことができる。

【００１１】公開鍵と秘密鍵とは１対１に対応し、秘密鍵から公開鍵を知ることは比較的容易であるが、公開鍵から秘密鍵を知ることは非常に困難であるように設計されている。さらに、公開鍵で暗号化したものは、対応する秘密鍵でしか復号できないし、秘密鍵で暗号化したものは、対応する公開鍵でしか復号できないように設計されている。

【００１２】本実施形態では、公開鍵暗号方式において、非対称の２つの鍵のうち一方の鍵を公開しておける点を利用し、公開鍵をディジタル署名として複写物中に埋め込むことで、複写物を見ること自体はできるが、その複写物をさらに複写しようとする際には対応する秘密鍵がなければ複写できないという、いわば「緩いセキュリティ」を複写物に設けるものである。

【００１３】以下、図面を参照して本実施形態について説明する。図１は、本発明の代表的な実施形態を示した図である。図１において、画像読み取り部１０１では、複写機の図示しない原稿台に置かれた原稿を照射し、その反射光をＣＣＤなどの光電変換素子上に結像させて画像情報を得る。このとき、光電変換素子は、Ｒ，Ｇ，Ｂそれぞれのカラーフィルタを通して１つずつの素子で受光し、３つの素子で１つの画素を構成する。なお、本明細書において画像とは、絵や写真等の静止画の他に文字や表、グラフ、数式など原稿に記録され得るあらゆる情報を言うものとする。

【００１４】入力画像処理部１０２は、読み取った画像情報に対して色味合わせ、シェーディング補正などの画像処理を施す。なお、画像処理を施す対象の画像情報は、ネットワーク１１３上からネットワークＩ／Ｆ１０９を介して送信されてくる画像データでも構わない。入力処理された画像信号は、出力画像処理部１０５に送られる。ここでは、ＲＧＢからＣＭＹＫへの表色系変換な

ど、紙面への出力に適した変換処理が施され、画像出力部１０６に出力される。

【００１５】画像出力部１０６では、受け取った画像信号に従って、１画素に対して１ドットずつトナーやインクなどを打ち込み、紙媒体上に画像を形成する。なお、操作部１０７は、例えばディスプレイパネルやタッチパネルによるキー操作によって上述の各ブロックの動作条件の指示、状態の表示を行う。

【００１６】暗号鍵検出部１０３では、複写物の画像信号に埋め込まれた暗号鍵（公開鍵）を検出する。公開鍵は、人間の目には目立ちにくいドットパターンとして画像中に埋め込まれたものであり、複写物の見ためには影響を及ぼさない程度の情報である。例えば、人間の目には目立ちにくい黄色いドットで複写物に打ち込んだものである。また、視覚には感度の無いような特殊なインクを用いて紙媒体に打ち込むヘッドを画像出力部１０６に用意し、そのような特殊なインクを打ち込んだ複写物を再複写しようとするときに、画像読み取り部１０１でその特殊なインクに対応するセンサを用いて公開鍵のドットパターンを検出するようにしても良い。

【００１７】この公開鍵のドットパターンは、原稿の複写動作時に暗号鍵画像生成部１１０が、操作部１０７から入力された公開鍵データを、図２のような例で示す８×８のドットパターンとして任意の場所に埋め込んで生成するものとする。８×８のマトリクスの外枠が全て“１”の値（黒塗りのドット）をとるようにすることで公開鍵のドットパターンの存在を示すものとし、その内側の６×６の各ドットが“０”または“１”の値をとるようにすれば、この公開鍵データに対応する秘密鍵データは、０から$2^{36}-1$までの範囲内の整数をとれる。

【００１８】非対称暗号鍵変換部１１１は、秘密鍵から公開鍵への変換処理を行う。具体的には、例えば、以下のような非線形関数

$y=4x(1-x)^2$ ……（式１）

の演算を繰り返し実行するようなものを用いる。すなわち、この（式１）で示す関数に、秘密鍵データの値を2^{36}で除算して０から１の範囲の実数にしたものを初期値x_0として与え、以下のように繰り返し計算を行う。

【００１９】

$y_1=4x_0(1-x_0)^2$

$y_2=4y_1(1-y_1)^2$

・・・・

$y_{100}=4y_{99}(1-y_{99})^2$

【００２０】このようにして求められたy_{100}の値に2^{36}を乗算し、得られたデータを公開鍵として設定する。このように変換を行えば、秘密鍵から求めた初期値x_0と公開鍵として用いる最終値y_{100}とは１対１に対応し、さらに、初期値x_0から最終値y_{100}を求めるのは容易だが、最終値y_{100}から初期値x_0を求めるのは事実上不可能である。

【００２１】暗号鍵データベース１１２は、上述のようにして秘密鍵から変換された公開鍵を当該秘密鍵とあわせて、図３の例のように公開鍵と秘密鍵との対応関係として記憶する。暗号鍵データベース１１２にデータを追加する際には、操作部１０７より秘密鍵データを入力し、非対称暗号鍵変換部１１１により変換された公開鍵データと共に追加することとする。

【００２２】暗号鍵照合部１０４は、原稿の複写動作時に暗号鍵検出部１０３で入力画像信号中から検出された公開鍵と、複写機からの問い合わせに応じてユーザが操作部１０７より入力した秘密鍵との組み合わせが暗号鍵データベース１１２に存在するかどうかを照合し、その照合結果に応じて画像出力の許可あるいは禁止を指示する制御信号を送出する。

【００２３】上述した各部は、複写機の内部バス１１４に接続され、制御部１０８によって制御される。制御部１０８は、例えばＲＡＭもしくはＲＯＭに記録されたプログラムに従って動作するＣＰＵにより構成される。

【００２４】図４は、図１に示した構成を用いて公開鍵を複写物に埋め込む際の動作を矢印付きで示すブロック図である。図４において、操作部１０７で公開鍵を複写物に埋め込むことを指示して複写動作を行うと、まず、暗号鍵データベース１１２は、既に登録されている公開鍵の一覧を操作部１０７に送る。

【００２５】操作部１０７は、ディスプレイパネルに公開鍵一覧を表示して、再複写動作を許可する相手の公開鍵の選択をユーザに要求する。これに対応してユーザにより選択された公開鍵は、暗号鍵画像生成部１１０に送られ、図２に示したような８×８のマトリクス画像に変換されて、出力画像処理部１０５に送られる。

【００２６】一方、画像読み取り部１０１で読み取られた原稿の画像信号は、入力画像処理部１０２で所定の画像処理が施され、出力画像処理部１０５に送られる。出力画像処理部１０５では、暗号鍵画像生成部１１０より供給された公開鍵のドットパターンと、入力画像処理部１０２より供給された原稿の画像信号とを画像出力部１０６に送って、紙媒体上に画像を出力することにより複写物を生成する。

【００２７】図５は、公開鍵が埋め込まれた複写物を再複写する際の動作（暗号鍵検出時の動作）を矢印付きで示すブロック図である。図５において、画像読み取り部１０１で読み取られた複写物の画像信号、またはネットワーク１１３上を送信され、ネットワークＩ／Ｆ１０９を介して読み込まれた画像信号は、入力画像処理部１０２で所定の画像処理が施され、出力画像処理部１０５および暗号鍵検出部１０３に送られる。

【００２８】暗号鍵検出部１０３では、入力された複写物の画像信号中から埋め込まれた暗号鍵（公開鍵）を検出する。暗号鍵が検出できなかった場合（暗号鍵が埋め込まれていなかった場合）は、自由に複写して良い文書

等なので、暗号鍵検出部１０３は出力画像処理部１０５にそのまま画像の出力を行わせるように制御信号を送る。一方、暗号鍵を検出した場合は、検出した暗号鍵を暗号鍵照合部１０４に送るとともに、操作部１０７のディスプレイパネルに所定の表示をすることにより、ユーザに秘密鍵の入力を要求する。

【００２９】ユーザにより秘密鍵が入力されると、その秘密鍵は暗号鍵照合部１０４に送られる。暗号鍵照合部１０４では、暗号鍵検出部１０３で検出した公開鍵と、操作部１０７より入力された秘密鍵との組み合わせが暗号鍵データベース１１２に存在するかどうかを照合する。その結果、あらかじめ登録されている暗号鍵の組み合わせが存在すれば、出力画像処理部１０５に画像出力を行わせるように制御信号を送る。

【００３０】一方、照合した結果があらかじめ登録されている暗号鍵の組み合わせの何れでもなかった場合には、出力画像処理部１０５に画像出力を禁止する制御信号を送ると同時に、操作部１０７に画像出力が認められない旨のメッセージを表示する。上記のような動作により、公開鍵が埋め込まれた複写物は、その復写物に誰の公開鍵が埋め込まれているかという情報と、その人物の秘密鍵の情報とが無ければ複写行為を行うことができないようになる。

【００３１】以上説明したように、本実施形態の構成によれば、コピー時に再コピーを許可したい特定の人間の公開鍵データを人間の目には目立ちにくい形で複写物に埋め込むため、何れの人間に対しても通常の複写物に同様に見えながらも、特定の人間以外には再コピーを禁止することができる。

【００３２】また、本実施形態の自然な拡張として、複数の公開鍵データを複写画像中に埋め込むことができ、この場合、複数の人間に対して複写行為を許可することができる。

【００３３】次に、本発明の第２の実施形態を説明する。第２の実施形態は、上述した第１の実施形態の構成を持つ複写機がネットワーク上に接続されている場合、ネットワーク上の全機器において、特定個人に対する複写行為の許可を行う例である。

【００３４】図６は、暗号鍵の情報をネットワーク上の各機器で共有するために用いられる暗号鍵パケット６０１の構成を示す図である。図６において、ヘッダ６０２は、ＩＳＯ階層での物理層からアプリケーション層までのヘッダを含むものとし、ネットワークアドレスおよび暗号鍵パケットであることを示す情報が入っている。また、暗号鍵情報６０３は、登録した秘密鍵の情報を含む。

【００３５】本実施形態では、ネットワーク上の複数の機器間で秘密鍵の情報をやり取りするため、暗号鍵情報６０３自体が暗号化されていることが好ましいが、ここではこの暗号化についての詳細な説明は省略する。なお、ネットワークプロトコルとしてはＴＣＰ／ＩＰなどが挙げられるが、特にその種類にはこだわらない。

【００３６】図７は、各複写機の動作を矢印付きで示すブロック図である。図７において、ネットワーク１１３上に送信された暗号鍵パケット６０１は、ネットワークＩ／Ｆ１０９で受信される。ネットワークＩ／Ｆ１０９は、受信した暗号鍵パケット６０１中のヘッダ６０２を解釈して、暗号鍵（秘密鍵）情報６０３を取り出し、非対称暗号鍵変換部１１１に渡す。

【００３７】非対称暗号鍵変換部１１１では、秘密鍵から公開鍵への一方向性関数を用いて変換を行い、得られた公開鍵を秘密鍵と共に暗号鍵データベース１１２に登録する。以上の動作は、ネットワーク１１３上の各複写機で行われるため、各複写機の暗号鍵データベース１１２は同一に保たれる。これ以外の動作は、上述した第１の実施形態と同様であるので、重複する説明を省略する。

【００３８】以上説明したように、第２の実施形態の構成によれば、ネットワーク１１３上に存在する各複写機が同一の暗号鍵データベース１１２を保持しているため、ネットワーク１１３上の複数の複写機において、特定の人間以外の複写行為を効果的に抑制することができる。

【００３９】なお、以上の実施形態では複写機を例とって説明したが、本発明の画像処理装置はこれに限定されるものではない。

【００４０】

【発明の効果】本発明は上述したように、非対称暗号方式に基づく一方の鍵を複写動作時に紙媒体上に人間の視覚には目立ちにくい形で埋め込むようにしたので、複写物を見ること自体はできるが、その複写物をさらに複写しようとする際には、埋め込まれた一方の鍵に対応する他方の鍵がなければ複写できないすることができ、何れの人間に対しても通常の複写物に同様に見えながらも、上記他方の鍵を有する特定の人間以外には再複写を禁止することができる。

【００４１】また、本発明の他の特徴によれば、上記のような画像処理装置をネットワーク上に接続した画像処理システムにおいて、上記他方の鍵の一例である秘密鍵をネットワーク上で送受信するように成し、ネットワークを介して外部より入力された秘密鍵を鍵変換手段に供給するようにしたので、外部より供給された秘密鍵も内部で入力された秘密鍵と同様に、対応する公開鍵と共に暗号鍵データベースに格納することができ、ネットワーク上にある複数の画像処理装置が同一の暗号鍵データベースを保持するようにできる。これにより、ネットワーク上の複数の画像処理装置において特定の人間以外の複写行為を効果的に抑制することができる。

【図面の簡単な説明】

【図１】本発明による画像処理装置の一実施形態である

9

複写機の構成を示すブロック図である。

【図２】複写画像中に埋め込む公開鍵のドットパターンの一例を示す図である。

【図３】暗号鍵データベースの一例を示す図である。

【図４】複写時の暗号鍵埋め込み動作を矢印によって示すブロック図である。

【図５】複写時の暗号鍵検出および画像出力許可／禁止動作を矢印によって示すブロック図である。

【図６】本発明の第２の実施形態で使用する暗号鍵パケットの構成の一例を示す図である。

【図７】暗号鍵パケット送受信時の動作を矢印によって示すブロック図である。

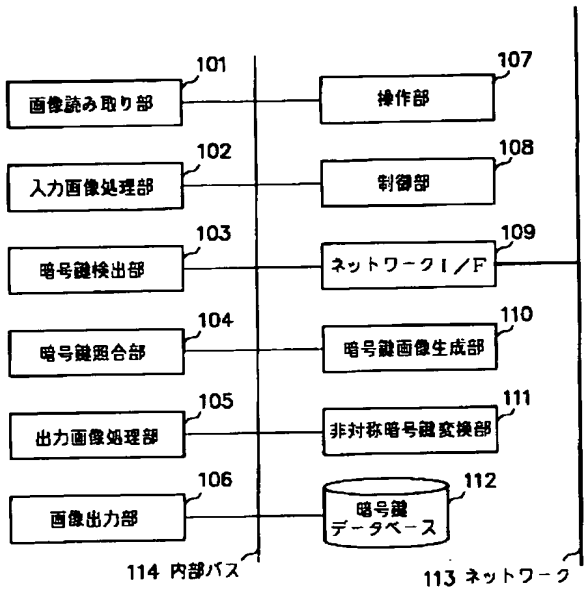
【符号の説明】

１０１　画像読み取り部
１０２　入力画像処理部

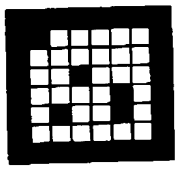
10

１０３　暗号鍵検出部
１０４　暗号鍵照合部
１０５　出力画像処理部
１０６　画像出力部
１０７　操作部
１０８　制御部
１０９　ネットワークＩ／Ｆ
１１０　暗号鍵画像生成部
１１１　非対称暗号鍵変換部
１１２　暗号鍵データベース
１１３　ネットワーク
１１４　内部バス
６０１　暗号鍵パケット
６０２　ヘッダ
６０３　暗号鍵情報

【図１】



【図２】

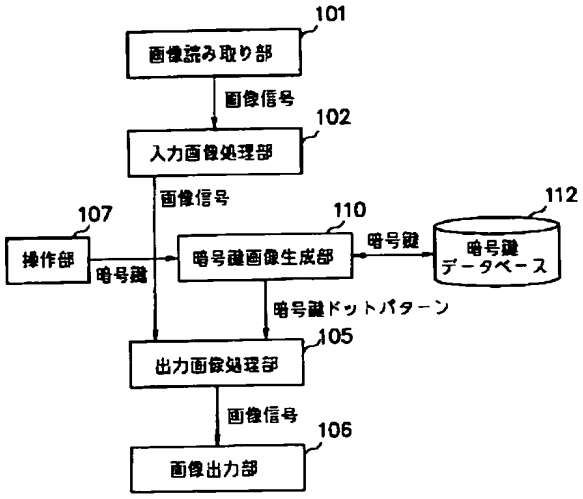


【図３】

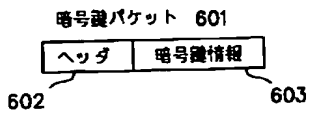
名前	公開鍵	秘密鍵
A	Ea	Da
B	Eb	Db
C	Ec	Dc
.	.	.
.	.	.
.	.	.

暗号鍵データベース

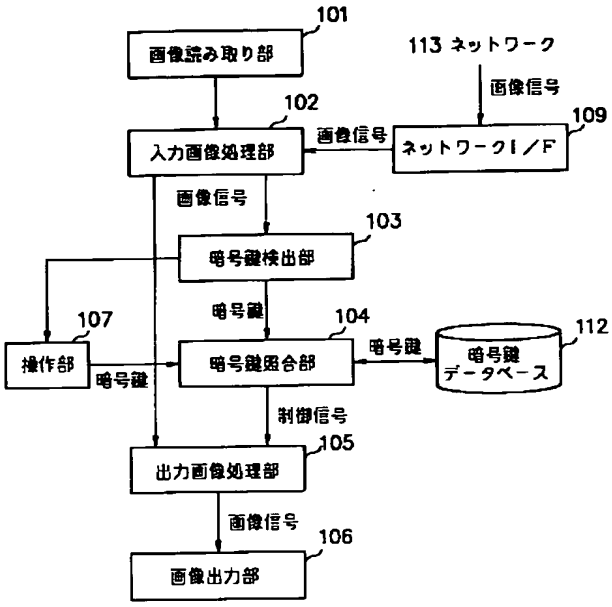
【図４】



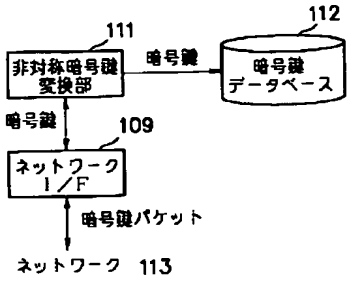
【図６】



【図５】



【図７】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
	5/00			5/00	
Ｈ０４Ｌ	9/32		Ｈ０４Ｎ	1/00	Ｃ
Ｈ０４Ｎ	1/00		Ｈ０４Ｌ	9/00	６７５Ｂ
	1/40		Ｈ０４Ｎ	1/40	Ｚ